CLAIMS

1. An information playback device for playing back information from a recording medium having encrypted content recorded thereon by a content recording entity, the information playback device comprising:

a cryptosystem unit operable to determine the validity of a public key certificate of the content recording entity, to acquire a public key of the content recording entity from the public key certificate if the public key certificate is valid, and to decrypt the encrypted content if the validity of a digital signature of the content recording entity is verified based on the acquired public key.

2. An information playback device according to Claim 1, wherein the digital signature of the content recording entity is generated by digitally signing the encrypted content, and the cryptosystem unit decrypts the encrypted content if the validity of the generated digital signature is verified.

3. An information playback device according to Claim 1, wherein the digital signature of the content recording entity is generated by digitally signing a title key which corresponds to the encrypted content, and the cryptosystem unit decrypts the encrypted content if the validity of the generated digital signature is verified.

4. An information playback device according to Claim 1, further comprising:

a plurality of nodes constituting a layered key-tree structure having a plurality of different information playback devices as leaves, the key-tree structure defining a plurality of node paths each including a multiplicity of the nodes arranged serially from a lowermost node to an uppermost node; and

a plurality of stored keys including node keys unique to the plurality of nodes and leaf keys unique to the plurality of different information playback devices;

wherein the cryptosystem unit is operable to acquire decryption-key-generating data required for decrypting the encrypted content by decrypting, based on the stored keys, an enabling key block composed of data generated by using each key on one node path to encrypt a next adjacent upper key on the one node path.

5. An information playback device according to Claim 4, wherein the decryption-key-generating data is a master key common to the plurality of different information playback devices or a media key unique to the recording medium.

6. An information recording device for recording information on a recording medium, the information recording device comprising:

a cryptosystem unit operable to encrypt content recorded on the recording medium by a content recording entity, to generate a digital signature of the content recording entity, and to record the encrypted content, the digital signature, and a public key certificate of the content recording entity on the recording medium so as to correspond to one another.

7. An information recording device according to Claim 6, further comprising:

a processing unit operable to generate a management table having correspondences among addresses of the encrypted content, the digital signature, and the public key certificate, and to record the management table on the recording medium.

8. An information recording device according to Claim 6, wherein the cryptosystem unit is operable to generate the digital signature of the content recording entity by digitally signing the encrypted content, and to record the generated digital signature in association with the encrypted content.

9. An information recording device according to Claim 6, wherein the cryptosystem unit is operable to generate the digital signature of the content recording entity by digitally signing a title key which corresponds to the encrypted content, and to record the generated digital signature in association with the encrypted content.

10. An information recording device according to Claim 6, further comprising:

a plurality of nodes constituting a layered key-tree structure having a plurality of different information playback devices as leaves, the key-tree structure defining a plurality of node paths each including a multiplicity of the nodes arranged serially from a lowermost node to an uppermost node; and

a plurality of stored keys including node keys unique to the plurality of nodes and leaf keys unique to the plurality of different information playback devices;

wherein the cryptosystem unit is operable to acquire encryption-key-generating data required for encrypting the content recorded on the recording medium by decrypting, based on the stored keys, an enabling key block composed of data generated by using each key in one node path to encrypt a next adjacent upper key on the one node path.

11. An information recording device according to Claim 10, wherein the encryption-key-generating data is a master key common to the plurality of different information playback devices or a media key unique to the recording medium.

12. A method for playing back information from a recording medium having encrypted content recorded thereon by a content recording entity, the method comprising:

determining the validity of a public key certificate of the content recording entity;

acquiring a public key of the content recording entity from the public key certificate if the public key certificate is valid;

verifying the validity of a digital signature of the content recording entity based on the acquired public key; and

decrypting the encrypted content if the validity of the digital signature is verified.

13. An information playback method according to Claim 12, further comprising:

generating the digital signature of the content recording entity by digitally signing the encrypted content, wherein the step of verifying the validity of the digital signature includes verifying the validity of the generated digital signature.

14. An information playback method according to Claim 12, further comprising:

generating the digital signature of the content recording entity by digitally signing a title key which corresponds to the encrypted content, wherein the step of verifying the validity of the digital signature includes verifying the validity of the generated digital signature.

15. An information playback method according to Claim 12, further comprising:

providing an information playback device having a plurality of nodes constituting a layered key-tree structure having a plurality of different information playback devices as leaves, the key-tree structure defining a plurality of node paths each including a multiplicity of the nodes arranged serially from a lowermost node to an uppermost node, and a plurality of stored keys including node keys unique to the plurality of nodes and leaf keys unique to the plurality of different information playback devices;

generating key data by using each key on one node path to encrypt a next adjacent upper key on the one node path; and

acquiring decryption-key-generating data required for decrypting the encrypted content by decrypting, based on the stored keys, an enabling key block composed of the key data.

16. A method for recording information on a recording medium, comprising:

encrypting content recorded on the recording medium by a content recording entity;

generating a digital signature of the content recording entity; and

recording the encrypted content, the digital signature, and a public key certificate of the content recording entity on the recording medium so as to correspond to one another.

17. An information recording method according to Claim 16, further comprising:

generating a management table having correspondences among addresses of the encrypted content, the digital signature, and the public key certificate; and

recording the management table on the recording medium.

18. An information recording method according to Claim 16, further comprising

generating the digital signature of the content recording entity by digitally signing the encrypted content; and

recording the generated digital signature on the recording medium in association with the encrypted content.

19. An information recording method according to Claim 16, further comprising:

generating the digital signature of the content recording entity by digitally signing a title key which corresponds to the encrypted content; and

recording the generated digital signature on the recording medium in association with the encrypted content.

20. An information recording method according to Claim 16, further comprising:

providing an information recording device having a plurality of nodes constituting a layered key-tree structure having a plurality of different information playback devices as leaves, the key-tree structure defining a plurality of node paths each including a multiplicity of the nodes arranged serially from a lowermost node to an uppermost node, and a plurality of stored keys including node keys unique to the plurality of nodes and leaf keys unique to the plurality of different information playback devices;

generating key data by using each key on one node path to encrypt a next adjacent upper key on the one adjacent node path; and

acquiring encryption-key-generating data required for encrypting the content recorded on the recording medium by decrypting, based on the stored keys, an enabling key block composed of the key data.

21. An information recording medium, comprising:

encrypted content recorded thereon by a content recording entity;

identification data for identifying the content recording entity;

a public key certificate of the content recording entity; and

a digital signature of the content recording entity.

22. An information recording medium according to Claim 21, further comprising:

a management table having correspondences among addresses of the encrypted content, the digital signature, and the public key certificate.

23. A program storage medium storing a computer program for controlling a computer system to execute a process for playing back information from a recording medium having encrypted content recorded thereon by a content recording entity, the computer program comprising:

determining the validity of a public key certificate of the content recording entity;

acquiring a public key of the content recording entity from the public key certificate if the public key certificate is valid;

verifying the validity of a digital signature of the content recording entity based on the acquired public key; and

decrypting the encrypted content if the validity of the digital signature is verified.

24. A program storage medium storing a computer program for controlling a computer system to execute a process for recording information on a recording medium, the computer program comprising:

encrypting content recorded on the recording medium by a content recording entity;

generating a digital signature of the content recording entity; and

recording the encrypted content, the digital signature, and a public key certificate of the content recording entity on the recording medium so as to correspond to one another.

25. An information playback device for playing back information from a recording medium having encrypted content recorded thereon by a content recording entity, the information playback device comprising:

a cryptosystem unit operable to acquire from the recording medium identification data representing the content recording entity, to determine a revocation state of the content recording entity based on the acquired identification data, and to decrypt the encrypted content if the content recording entity has not been revoked.

26. An information playback device according to Claim 25, wherein the cryptosystem unit is operable to determine the validity of a public key certificate of the content recording entity, to acquire data identifying the content recording entity from the public key certificate if the public key certificate is valid, and to determine whether the content recording entity has been revoked based on the identifying data.

27. An information playback device according to Claim 25, wherein the cryptosystem unit is operable to decrypt

the encrypted content if the validity of a digital signature of the content recording entity is verified.

28. An information playback device according to Claim 25, wherein the cryptosystem unit is operable to determine the validity of a public key certificate of the content recording entity, to acquire a public key of the content recording entity from the public key certificate if the public key certificate is valid, and to decrypt the encrypted content if the validity of a digital signature of the content recording entity is verified based on the public key.

29. An information playback device according to Claim 25, wherein the cryptosystem unit is operable to determine the validity of a digital signature of the content recording entity generated by digitally signing the encrypted content, and to decrypt the encrypted content if the digital signature is valid.

30. An information playback device according to Claim 25, wherein the cryptosystem unit is operable to determine the validity of a digital signature of the content recording entity generated by digitally signing a title key corresponding to the encrypted content, and to decrypt the encrypted content if the digital signature is valid.

31. An information playback device according to Claim 25, wherein the cryptosystem unit is operable to determine the validity of a public key certificate of the

content recording entity, to acquire data identifying the content recording entity from the public key certificate if the public certificate is valid, and to determine whether the content recording entity has been revoked based on a comparison between the identifying data and an identification stored in a revocation list.

32. An information playback device according to Claim 25, further comprising:

a layered key-tree structure having a plurality of devices as leaves, the key-tree structure defining a plurality of paths each including a root, nodes and the leaves arranged serially from the root to an end leaf, each of the root, nodes and leaves corresponding to a unique key,

wherein the cryptosystem unit is operable to determine the validity of a public key certificate of the content recording entity, to acquire data identifying the content recording entity from the public key certificate if the public key certificate is valid, and to determine whether the content recording entity has been revoked by executing a process, based on the identifying data, of following the indices of an enabling key block composed of data generated by using each of the keys on a selected path to encrypt a next adjacent upper key on the selected path.

33. An information playback device according to Claim 25, further comprising:

a plurality of nodes constituting a layered key-tree structure having a plurality of different information playback devices as leaves, the key-tree structure defining a plurality of node paths each including a multiplicity of the nodes arranged serially from a lowermost node to an uppermost node; and

a plurality of stored keys including node keys unique to the plurality of nodes;

wherein the cryptosystem unit is operable to acquire decryption-key-generating data required for decrypting the encrypted content by decrypting, based on one of the stored keys, an enabling key block composed of data generated by using each of the keys on one node path to encrypt a next adjacent upper key on the one node path.

34. An information playback device according to Claim 33, wherein the decryption-key-generating data is a master key common to the plurality of different information playback devices or a media key unique to the recording medium.

35. A method for playing back information from a recording medium having encrypted content recorded thereon by a content recording entity, the method comprising:

acquiring from the recording medium identification data representing the content recording entity;

determining a revocation state of the content recording entity based on the acquired identification data; and

decrypting the encrypted content if the content recording entity has not been revoked.

36. An information playback method according to Claim 35, further comprising:

determining the validity of a public key certificate of the content recording entity;

acquiring data identifying the content recording entity from the public key certificate if the public key certificate is valid; and

determining whether the content recording entity has been revoked based on the identifying data.

37. An information playback method according to Claim 35, further comprising:

verifying the validity of a digital signature of the content recording entity; and

decrypting the encrypted content if the validity of the digital signature is verified.

38. An information playback method according to Claim 35, further comprising:

determining the validity of a public key certificate of the content recording entity;

acquiring a public key of the content recording entity from the public key certificate if the public key certificate is valid;

verifying the validity of a digital signature of the content recording entity based on the public key; and

decrypting the encrypted content if the validity of the digital signature is verified.

39. An information playback method according to Claim 35, further comprising:

verifying the validity of a digital signature of the content recording entity generated by digitally signing the encrypted content; and

decrypting the encrypted content if the digital signature is valid.

40. An information playback method according to Claim 35, further comprising:

verifying the validity of a digital signature of the content recording entity generated by digitally signing a title key corresponding to the encrypted content; and

decrypting the encrypted content if the digital signature is valid.

41. An information playback method according to Claim 35, further comprising:

determining the validity of a public key certificate of the content recording entity;

acquiring data identifying the content recording entity from the public key certificate if the public key certificate is valid; and

determining whether the content recording entity has been revoked based on a comparison between the identifying data and an identification stored in a revocation list.

42. An information playback method according to Claim 35, further comprising:

providing an information playback device having a layered key-tree structure having a plurality of devices as leaves, the key-tree structure defining a plurality of paths each including a root, nodes and the leaves arranged serially from the root to an end leaf, each of the root, nodes and leaves corresponding to a unique key;

determining the validity of a public key certificate of the content recording entity;

acquiring data identifying the content recording entity from the public key certificate if the public key certificate is valid; and

determining whether the content recording device has been revoked by executing a process, based on the identifying data, of following the indices of an enabling key block composed of data generated by using each of the keys on a selected path to encrypt a next adjacent upper key on the selected path.

43. An information playback method according to Claim 35, further comprising:

providing an information playback device having a plurality of nodes constituting a layered key-tree structure having a plurality of different information playback devices as leaves, and a plurality of stored keys including node keys unique to the plurality of nodes and leaf keys unique to the plurality of nodes; and

acquiring decryption-key-generating data for decrypting the encrypted content by decrypting an enabling key block based on the stored keys.

44. An information recording medium, comprising:

encrypted content recorded thereon by a content recording entity;

a public key certificate for the content recording entity;

a digital signature of the content recording entity; and

a revocation list.

45. An information recording medium according to Claim 44, further comprising:

a management table having correspondences among addresses of the encrypted content, the digital signature, and the public key certificate.

46. A program storage medium storing a computer program for controlling a computer system to execute a process

for playing back information from a recording medium having encrypted content recorded thereon by a content recording entity, the computer program comprising:

acquiring from the recording medium identification data representing the content recording entity;

determining a revocation state of the content recording entity based on the acquired identification data; and

decrypting the encrypted content if the content recording entity has not been revoked.